

**SYSTEM AND METHOD FOR PROVIDING CUSTOMERS WITH
SEAMLESS ENTRY TO A REMOTE SERVER**

CROSS REFERENCE TO RELATED APPLICATIONS

This application is a continuation in part of application serial number 09/ 591,687
5 filed on June 12, 2000, entitled "System and Method for Providing Customers With
Seamless Entry to A Remote Server, and which is incorporated herein by reference for
all purposes.

FIELD OF THE INVENTION

The present invention relates to a method that provides customers of a host
10 service provider or host server with a seamless experience, allowing them to access
remote network services, which typically require their own username, password, and
session management application, via a single login to the host service provider.

BACKGROUND OF THE INVENTION

A network service provider may want to provide its customers with access to
15 services that are not provided directly by its server. Therefore, the service provider may
have to redirect its customers to another remote server capable of providing the service.

For example, an Internet banking site may wish to provide its customers with a
full range of banking services, e.g., opening and maintaining a checking account,
applying for a credit card or loan, paying bills, or accessing brokerage or financial
20 planning services. Each of these Internet banking services may be provided by an
independent server that requires the user to enter a unique username (or ID) and
password. Therefore, when a customer wishes to utilize a banking service that is

provided by a remote server, after the Internet banking host server redirects the customer to the remote service provider, the customer must enter a new username and password specific to that service. Given the broad range of services that an Internet bank may wish to provide, this places the burden of remembering and entering multiple usernames and passwords on the customer. This is a significant drawback to the customer. This is also a significant drawback to the Internet bank because customer dissatisfaction may result in lost accounts.

Furthermore, if the customer returns to the host provider after accessing a remote service provider, and then desires to return to the remote service provider, the customer must re-enter the same username and password for that service. For example, in the Internet banking context, if a customer decides to access his or her checking account, then utilize brokerage services, and then desires to return to his or her checking account, the customer must enter his or her unique username and password for the checking account service twice. This is a significant drawback.

In addition, a host service provider may wish to change the remote service providers that customers can access through its server. In the Internet banking context, for example, a host Internet bank may utilize a particular remote service to provide its customers with checking account services. For different reasons, the host Internet bank may later wish to change the remote checking account service provider. This would require the Internet banking customer to create and remember a new username and password for the new remote service. Again, the burden of remembering an even greater number of user names and passwords falls on the customer and the risk of losing those customers is borne by the host Internet bank. This is another significant drawback.

Other drawbacks to conventional approaches exist.

SUMMARY OF THE INVENTION

The present invention overcoming these and other drawbacks of existing systems relates to a system and method for providing customers with seamless entry to a remote server, in which a mediation engine coordinates access to multiple network sites without
5 a need for continuous reentry of user ID or other information.

One feature of the present invention is to provide a specific time limit which a user can spend logged into the system.

Another feature of the present invention is to monitor the state of a user to determine whether the user is logged in or not.

10 Another feature of the present invention is to provide customers of a host service provider with a seamless experience enabling them to gain access to one or more remote services by entering a single username and password required by the host service provider.

15 Another feature of the invention is to enable customers of a host service provider to regain access to a remote service provider, after having exited that remote server, without having to re-enter the username and password required by that remote service provider.

20 Another feature of the invention is to enable a host service provider to replace or add remote services that a customer can access through the host service provider without placing the additional burden on customers to enter a new username and password.

Another feature of the present invention is to provide an on-line banking service having a consolidated financial homepage that gives customers a read-only summary of information on all accounts they currently have with the banking service as well as value-add features like stock portfolio, personal reminders and targeted news feeds.

Another feature of the present invention may include the capability to personalize the web site based on customer information and preferences.

Yet another feature of the present invention may include the ability for customers to bookmark pages inside of the on-line bank, and access those pages directly without
5 accessing a homepage.

These and other features of the invention will become apparent to persons skilled in this art from the following description.

One aspect of the present invention provides a seamless entry banking system for offering a plurality of financial products and services to customers via a single login.

10 The banking system comprises a host server, at least one remote server, a universal session manager, and a validation module operatively linked through an electronic network. The universal session manager and validation module enable customers of the banking system to access the host server and a remote server via a single login either to the host server or a remote server. For example customers (or users) may connect to a
15 host service provider module using a unique username and password. Then, through a series of data exchanges, or handshakes, between the universal session manager, the validation module database, and a remote server, the customer may be transparently logged into the remote server or service provider. The universal session manager and/or the validation database may be a part of the host server service module or alternatively
20 may be operated independently of the host server.

Customers may utilize a browser system to connect to the banking system. The banking system may provide a range of banking services including on-line bill paying, instant credit card applications, loan applications, online automated clearinghouse

(ACH), or checking account services. Each service may be supported by the host server or a remote or distinct server that is operatively linked to the host server.

Another aspect of the present invention relates to a method for accessing a plurality of financial services and products that are offered by a banking system comprising a host server and a plurality of remote servers operatively linked across an electronic network. The method includes receiving login information for accessing the host server from a customer of the banking system and retrieving data for accessing at least one remote server based at least in part on the received login information. The method further includes transmitting the retrieved data to the at least one remote server thus allowing the customer to transparently gain access to the remote server.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 depicts a schematic diagram of a system, according to an embodiment of the present invention.

Figures 2A and 2B depict a flow diagram illustrating a method, according to an embodiment of the present invention.

Figures 3A and 3B depict an exemplary graphical user interface, according to an embodiment of the present invention.

Figure 4 shows one embodiment of a web site, according to an embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

For purposes of illustration, a system and method according to a preferred embodiment of the present invention are described herein. The system is described as being part of an Internet based system that enables customers of an Internet banking

system to access remote Internet banking services, which may require a unique username and password, having only entered a single username and password required by the host Internet banking system. Furthermore, the invention is described in terms of an Internet based bank providing a multitude of financial services, some of which are provided by remote providers. However, it should be appreciated that this embodiment is exemplary only and that the invention finds application in any scenario involving a host site that includes links to distinct remote sites with their own separate login procedures. It should also be appreciated that the present invention could be implemented through a variety of networks such as a telephone network, a satellite connection network, or other network.

Also, for illustration purposes only, the invention is described in terms of the existing Internet. The skilled artisan will recognize that the invention could be implemented in variations thereto, such as the so-called Internet Protocol Next Generation (IPng) or any other variations of networked packet-switched technology.

According to one illustrative embodiment of the method of the present invention, a customer may first enter a username and password to gain access to the host server of an Internet bank. During the connection to the host server, a validation module validates the customer's username and password. If the combination is valid, the validation module transmits data to a universal session manager indicating which services the customer is enrolled in and the unique username and password that have been generated for each remote service in which the customer is enrolled. The customer is then free to select one of these remote services provided by a remote server through a link provided by the host service provider. For example, if a customer chooses to complete a loan application and this service is provided by a remote server requiring its own user ID and

password, the universal session manager may then pass the required user ID and password to the remote server's login module.

The remote server may receive the data required for login, from the universal session manager and transmit to the universal session manager the status of the login attempt. If the login is successful, the customer may utilize the remote service with his/her web browser system without having to enter a username or password particular to the remote service.

In another illustrative embodiment, the present invention may provide customers of a banking system with access to remote service providers which require their own unique user IDs and passwords and have other special access requirements. For example, a customer may utilize a browser system to connect to a network bank providing a range of banking services with special access requirements. These secure services may include brokerage services. If after entering a valid username and password to the host service provider the customer chooses to utilize a remote brokerage service provider with special access requirements, a trusted server may act as an intermediary between the universal session manager of the host server and the remote brokerage system, for example. The trusted server may answer the login request of the banking site's universal session manager with a session ID extracted from a cookie placed on the user's browser by the trusted server. When the universal session manager receives the session ID, the customer may be redirected to the remote brokerage site.

Referring to Figure 1, an exemplary embodiment of the present invention system is illustrative. A plurality of users or customers 20 may be connected using a network 10 to a host service module or provider 50. For example the host service provider 50 may be an Internet banking service site. Network 10 also may comprise a cable network, a

LAN, a WAN, an intranet, an extranet, the Supernet, or any other electronic network that allows transmission of information.

Host service provider 50 may include a plurality of modules that function to perform the functions described above in addition to other functions set forth below.

5 Although separate modules are described for performing these functions, it should be understood that additional modules may also be provided and that modules may be combined.

According to an embodiment of the invention, host service provider 50 may comprise a universal session module or manager 52 and a validation database 60. The
10 universal session manager 52 may communicate with one or more databases 60 in communication with the host service provider 50. The database(s) 60 may store information required for login to remote sites or registration for the services those sites provide. Remote service provider 30 may comprise a registration module 32 and a login module 34. Registration module 32 may receive data from the universal session
15 manager 52 necessary for customer 20 registration with the remote service provider 30. Login module 34 may communicate with the universal session manager to receive the information required for access to the remote service provider, e.g., username and password. Login module 34 may also reply to the universal session manager 52 indicating the status of the login request.

20 The system may also include a trusted service module 70 and a trusted service provider 80. The trusted service module 70 acts as an intermediary between the universal session manager 52 and the trusted service provider 80. The trusted service provider 80 may be a remote service with special access requirements in addition to a unique username and password.

Referring now to Figures 2A and 2B, a method for providing customers with seamless entry to a remote server is illustrative. According to the method, a customer 20 employing a browser 22 may contact a host server such as an Internet banking service provider 50, according to block 125. A customer then transmits a personal username and password to a universal session manager 52 of the host service provider 50, according to block 150. The host service provider 50 may comprise a server system connected over a wide area network such as the World Wide Web or Internet 10 to provide web-pages upon request from one or more users utilizing a web browser 22. For example, a customer may use a browser 22 to connect over the Internet 10 to a web-site that provides Internet banking services. Existing browser/server technology may be used to transmit the username and password to the host service provider 50.

In response to the customer's transmitting a username and password to the universal session manager 52, the universal session manager 52 of the host service provider 50 may transmit the username and an encrypted version of the password to the validation database 60, according to block 200. The validation database 60 checks the username and password to make sure that the user has entered a valid username/password combination. If the username is not recognized by the validation database 60, according to block 325, or if the username and password do not match, according to block 350, the user will be asked to re-enter his or her username and password, according to block 150. The customer 20 of the Internet banking system 50 of Figure 1 may be allowed, for example, three or another number of attempts to enter a correct username ID/password combination. Once the customer 20 has entered a valid login, according to block 300, the database 60 will return to the universal session manager 52 the information necessary for the transparent login to the remote service 30,

according to block 400. As described, the information may comprise the type of the Internet banking services in which the customer 20 is enrolled and/or the username particular to that user and required by a remote banking service web site. The information may also in one embodiment include identifying information necessary for secured e-mail. The information also may include data necessary for profiling a dynamic application form related to user-selected products and services. The customer may select a link to one of the remote services 30 provided through the host service provider 50, according to block 450. For an Internet based banking system, these services may include, for example, checking account maintenance, credit card and loan applications services, electronic bill paying, and brokerage services. These services also may include Internet search engines, other web sites that offer membership services, e-mail services, or campaign advertising.

The universal session manager 52 may then check the validation database 60 return data to see if the customer has enrolled in the service, according to block 500. If the customer is enrolled in the selected service, the present embodiment initiates a triple handshake protocol, according to block 600. In the first step 625 of the triple handshake protocol 600, the universal session manager 52 may send the required customer username and password to the login module 34 of the remote service provider. This may comprise the universal session manager 52 of an Internet banking service provider 50 sending redirects to remote service web sites 30, which may include services such as on-line checking, on-line brokerage, on-line credit card application or online bill paying sites.

In the second step 650 of the triple handshake protocol 600, the login module 34 of the remote service module 30 sends the universal session manager 52 a reply

indicating the status of the login request. The status may indicate that the login attempt to the remote service provider 30 was successful according to block 725, or that the login attempt failed according to block 675, or that the login status is unknown, i.e., customer has never registered for the service before, according to block 700. For example the login module 34 may send redirects over the Internet 10 to the universal session manager 52 of the host Internet banking provider's web site 50.

In the final step 750 of the triple handshake protocol 600, the universal session manager 52 may direct the customer to a remote service provider 30. For example, the universal session manager 52 of an Internet banking web site 50 may redirect a customer to the web site of the selected remote service provider 30.

If the universal session manager 52 determines that the customer is not registered for the selected service the universal session manager 52 will transparently register the customer for that service, according to the no branch of block 500. Transparent registration may involve that the universal session manager 52 contact the validation database 60 to retrieve the information necessary for registration, according to block 525. This may include providing a unique username and password designated for use only with the selected service. Then the universal session manager 52 sends data to the registration module 32 of the remote service provider's web site, according to block 550. The remote service 30 then confirms the customer's registration, according to block 575 and the universal session manager 52 initiates the triple handshake protocol 600. In the present embodiment, transparent registration may be accomplished by a series of redirects between the universal session manager 52, the validation database 60, and the registration module 32 of the remote service provider 30.

The customer also may choose an Internet banking service, e.g., a brokerage service, that has special access requirements in addition to a unique username and password. If the customer is enrolled in the selected service, the system may initiate a trusted server dedicated line redirection.

5 For example, the trusted service module 70 can make a direct call to the trusted service provider 80, according to block 800. This may comprise a trusted brokerage server 70 established by an Internet banking service 50 providing a secure brokerage service 80 which the login redirects over a dedicated line. The trusted service provider 80 may respond to the trusted service module 70 in the form of an html response with a
10 session ID associated with it, according to block 825. For example, this may involve a brokerage system 80 responding to a trusted brokerage server 70 in html form over a dedicated line. The trusted service module 70 may send this "cookie" to the user's network data acquisition module 22, after reading the session "cookie" and extracting session ID. For example, this may include a trusted brokerage server 70 placing this
15 "cookie" on the customer's Internet browser 22.

The trusted service module 70 next answers the universal session manager 52 with the status of the login attempt and the sessionID extracted from the cookie. Once the universal session manager 52 receives this data, if the login attempt was successful, the customer will be directed to the trusted service provider 80, as in step 750. This may
20 comprise, the universal session manager 52 of an Internet banking service provider 30 receiving data from a trusted brokerage server 70 and then redirecting the Internet banking customer 20 to a brokerage service provider 80.

During a session, if a customer 20 remains logged in, but no activity occurs, the universal session manager 52 performs a data security function by causing customer 20

to automatically logout. In a preferred embodiment, this timeout occurs after about thirty minutes of inactivity.

Figs. 3A and 3B illustrate an exemplary graphical user interface. Fig. 3A illustrates a screen that may be provided when a user 20 initially attempts to access host server 50. The user 20 is prompted to enter a user name and password, or alternatively to create a new user name and password to be granted seamless access to pertinent applications.

If the user 20 elects to create a new user name and password, access is granted upon the user's submission of data requested in Fig. 3B.

According to a preferred embodiment of the present invention an Internet Banking System is provided for offering many financial products or services to customers via a single sign-on process. The Internet Banking System comprises a host server that includes a Universal Session Manager (USM) for maintaining the customer single sign-on process. The USM is operatively linked to a validation database or module comprising a plurality of user profile databases. The USM authenticates a customer's login information and subsequently transparently logs the user into the various other services a customer has signed up for. Optionally, the USM may navigate a customer to various marketing, demonstration or application locations through the site of the Internet Banking host server. Preferably, authentication, customer-registration, customization of branded graphics, and ad generation are accomplished via one or more different modules operatively linked to the USM, however, it should be understood that these functions can also be accomplished via the USM. Separating these functions from the USM improves the overall functionality of the USM stream-lines the USM, and

creates a series of financial services that are readily accessible to a customer via the USM.

The Internet banking system may offer many financial products and services, some of which may be offered by remote service providers. Preferably the system may offer a consolidated homepage that provides an overview of all the available services that can be accessed via a single sign-on. The consolidated homepage may give a customer a read-only summary of information on all active accounts with the Internet banking service as well as value-add features like stock portfolio, personal reminders, and targeted news feeds. Also, preferably, the home page may be customizable by the customer to show only those accounts, information and views the customer wishes to have displayed upon successful login. For example, the homepage may include one or more of the following features:

- Bank account summary data presented on a secure homepage with applicable links;
- Account summaries for all Internet banking products on a single page;
- Customized stock portfolio tracking through an investment services module;
- Financial news feed;
- At your request offers;
- Personalization of the consolidated page to allow customers to choose what account summaries they want data displayed;
- Targeted promotions and advertising based on profiles of the customer;
- Targeted financial news feed based on customer's preferences;
- Reminder Service display of currently scheduled reminders; and

- Automated clearinghouse (ACH), which is an electronic network for permitting clearance of paper checks and transmitting information regularly between a bank and the Federal Reserve.

To accommodate the requirements for the consolidated homepage, various
5 services may be utilized, such as a dynamic page generator, a customer profile, an ad generator, or any other useful services.

The system may also allow card-members to see their credit card statements on the web site, and to have access to a bill pay functionality. Customers may also apply for credit cards or other financial transaction cards on-line. Customers having active card
10 accounts may view their card statement on the web site. For example a customer may use a username and password for logging to the host service provider web site and access their active credit card accounts.

Customers may also apply for other services offered by the host service provider or other remote service provider. Therefore, using a single login customers may access a
15 variety of services that would otherwise require multiple logins. The system will maintain the login information such as a username and password at one place and automatically update the login information whenever a customer changes this information for example by changing his or her password.

Preferably, the system may include a USM for controlling access to all Internet
20 services linked to the host server. The USM may employ one or more conventional procedures for authenticating the identity of a customer by employing one or more well known techniques, such as username/password rules, encryption technology, enrollment processes, question/answer techniques, etc. The USM may include at least one storage device or module or database for storing and maintaining primary login and

authentication information. Primary key mapping may occur depending upon the selected service, but does not necessarily exist universally. Customers may be notified, for example, via banner ads, emails, etc. about the consolidated login feature. Also, the login data may be duplicated in the profile database periodically to ensure continuity.

5 The primary function of the USM is to authenticate users, via a remote procedure call (RPC) to the validation module, and then transparently log them into the various services based on the remote services data sent back to the USM from the validation module via this RPC. The location of the USM may vary. For example, the USM may be part of the host server or it may be operated independently.

10 The on-line banking functions presented according to the invention may have a consistent look and feel to provide a consistent interface for a more customer friendly experience. For example, in one embodiment the top navigation bar may be reduced to the following tabs, Accounts, Products & Services, and Planning. When selecting the Products & Services tab, the customer will be presented with a page listing the banking
15 products and services they are entitled to have, but don't currently have. When a customer selects the Accounts tab, the customer will be directed to a page listing customer accounts. The planning tab may allow a user to plan a banking strategy.

The system may dynamically generate the site based on customer data, customer preferences, and where the customer is coming from, i.e., what link brought them to the

20 On-line Internet Bank. The types of variable aspects of the site generation may include, what services to show, for example, what pages to prepare, and which brand to show. For example, in order to dynamically show the services, to do targeted marketing, and to do private labeling, etc. the system may include a dynamic site assembler that can build

the site/pages dynamically based on predefined business rules, and a customer data and preferences.

The invention may include the capability to personalize the web site based on customer information and preferences. This may include dynamically determining what offers to target to customers depending on their personal data, e.g., profile, preferences, customer activity, and customer account data. It may also include dynamically determining what products to cross-sell to customers depending on their personal data.

Customers may also be given an option to bookmark pages inside of the on-line bank, instead of always taking them to the homepage. For example, this functionality may include displaying actual URL's in the browser's top URL display window and sending customers that haven't logged in to a different non-public homepage, instead of a public homepage non-customers view.

The system may also provide a frequently asked questions page with links to information sources. The system may also include a pricing service offering different price points.

According to one embodiment, shown in Figure 4, the Internet Banking system may comprises a web site including at least three frames, a global outer frame 401, a top frame or Top Navigation Bar 403 which contains links to the various internal services as well as Login/Logout buttons and a bottom frame 405, where the remote (external) services will be hosted. Inside the bottom frame, there can be up to two frames, one left-hand service specific navigation bar 405a and a main frame 405b hosting the page. The USM will maintain the global outer frame and the top navigation bar, transparently logging and directing the customers to the selected service whether via tab selections or

browser resize/refreshing. Also there may be left-hand navigation bars added (not shown).

The USM may typically update the last accessed times (LAT) and perform session timeouts based on this time variable. Activity in the top navigation bar and/or direct links to the dispatch servlet updating the LAT variables, thus preventing the customer sessions from timing out and being automatically logged out. If a customer is active within the bottom frame for more than a predetermined amount of time, such as 30 minutes (and does not activate the USM), their session may be closed and they will be logged out.

EXAMPLES:

Example 1 - Customer Login Specification

According to one embodiment of the present invention the host server may retrieve customer information data from a file in the validation module containing a plurality of customer login information and data. This file will contain authentication status and, if the status equals 0 for SUCCESS, it will contain the data necessary for the transparent logins to the various remote services in name-value pair format.

For example, the specification may include:

Customer login RPC input parameters:

- CIFAUTH.USERID1=userid
- CIFAUTH.PASSWORD=encrypted password

The validation module RPC will begin authentication of the customer. Possible return statuses include:

- STATUS=0 successful authentication (additional customer info will also be provided)
- STATUS=1 customer not found

- STATUS=2 authentication failure
- STATUS=3 authentication failure, exceeded max tries

Any status other than 0 (success) will return only the name STATUS and its value.

5 A success will return the following in a single, pipe-delimited, name-value pair string:

- STATUS=0
- CIF.ACN=customer number
- CIFAUTH.USERID1=userid
- CIFAUTH.PASSWORD=password
- CIFAUTH.LSTLOGDT=last successful login date
- CIFAUTH.LSTLOGTM=last successful login time
- CIF.TAXID=taxid
- CIF.FNAME=first name
- CIF.LNAME=last name
- CIF.EMAIL=email

repeated section for each service a customer has enrolled in:

- CIFSERV.SRVCAT=service category
(BROKER, PAYMENTS, CREDIT, LOANS, DEPOSITS, ECOMMERCE)
 - CIFSERV.SERVICE=service name (for category PAYMENTS, TRAVELERS)
 - CIFSERV.STATUS=numeric status field, complies to following business logic if more than one account. If at least one account has a CIFACCT.STATUS of 1 or 7, then set CIFSERV.STATUS to 1, else if at least one of the accounts has a CIFACCT.STATUS of 3, 4, or 8, then set CIFSERV.STATUS to 2, else set CIFSERV.STATUS to 0.
- | | | | | | | | | |
|---|---|---------|-------|-----|----------|----|-----|----------|
| 0 | - | account | open, | but | customer | is | not | enrolled |
| 1 | - | | | | active | | | account |
| 2 | - | | | | pending | | | account |

- CIFSERV.PASSWORD=password associated with this service

35 Each data pair will be delimited with a symbol such as a “|”. This architecture supports an unlimited number of services a customer may be linked to. If a customer has multiple accounts with a given service, the CIFSERV.STATUS will indicate the

customer's status with a service, not a single accounts' status. Thus, if a customer has at least one account with an active status, the CIFSERV.STATUS will be set to 1, else if they have at least one account with a pending status, the CIFSERV.STATUS will be set to 2, otherwise it will be set to 0. Essentially, the combination of two fields, SRVCAT and SERVICE, will repeat N times, depending on what services the customer has accounts with. Data needed for login for remote services can come from the non-recurring as well as the recurring sections. But it has to be data that is returned by the customer login procedure call.

Example 2 - Selecting a Service Tab/Link (Navigation)

According to a preferred embodiment, when a customer selects one of the service buttons or tabs on the top navigation bar (Figure 4), the USM may first check to see:

- (a) if the customer has been authenticated to the host server.
- (b) then it will check the validation module customer login RPC return data to see if the customer has enrolled in this service and depending on the

CIFSERV.STATUS value the USM will provide different behaviors for the customer as described below.

If (a) is false or if the CIFSERV.STATUS value is equal to 0 (not active), the USM will direct the customer to the services' demo/marketing/apply pages. Otherwise if the CIFSERV.STATUS value is equal to 2 (pending), the USM will redirect the customer to a generic message screen with the message, "Your application is being processed. You will be notified when your account is activated." Else if the CIFSERV.STATUS value is equal to 1 (active), the USM will check the customer's session activity table to see if they already logged into this service during their current

Internet Banking session. If they have, they will be redirected to the remote services “main” page, otherwise they will be redirected to the remote Services “login” handshake.

In this embodiment there may be two mechanisms in place to handle the triple handshake protocol. The first is a series of browser redirects, and the second uses a

5 Trusted Server with a dedicated line connecting Internet Banking system to the remote service. Those services requiring a dedicated line will use the Trusted Server to handle the transparent login of a customer to that remote service. Using the Trusted Server, once the transparent connection is completed successfully, a cookie may be placed on the person’s browser identifying the customer to that remote service and they are redirected
10 to the “main” page over the Internet.

The login parameters at the various remote services may vary. Some may require userid/password, some may require more parameters, less parameters, or different parameters. The USM preferably may be designed to accommodate any variety of login parameter required, as long as the parameters are stored at the validation module and are
15 returned to the USM from the validation module during the customer login RPC. The USM has the login properties identified in the usm.properties file. When new remote services are added or login requirements change, the new service needs to be specified in this file and the list of login parameters specified. This file may contain a listing of the validation module variable names and a mapping of the validation module names to the
20 variable names used by the USM.

Example 3 - “Single” or first leg of the “Triple” Handshake specification.

The USM may utilize dispatch and listen servlets to send redirects to the remote services. Redirection may include a “single” a “triple handshake” or a “tripleD” handshake. The “tripleD” is identical to the “triple” handshake, except that prior to

sending the browser redirects, the data will be encrypted with a DES algorithm. For example, the first leg of the “triple handshake” may have the following format:

5 https://<service_url>.com/login?<login_param_name1>=<login_id>&<login_param_name2>=<login_pwd>&returnURL=www.Internetbank.com/listen?action=login&USMid=<USMsessionId>&service=<service_name>

An example of this is:

https://banking.Internetbank.com/Scripts/bankstart.exe?userid=12345678&password=abcd4567897qr&returnURL=www.Internetbank.com/listen?action=login&USMid=99999&service=BANKING

10 The USM may have a configuration file/table containing service names and name specification of login values.

Each name-value pair may be unique in order to differentiate them. The designated names for the login values in the usm.properties file may be:

- 15
 - CIF.ACN = customer_userid
 - CIFAUTH.USERID1 = userid
 - CIFAUTH.PASSWORD = password
 - CIF.TAXID = taxid
 - CIF.FNAME = fname
 - CIF.LNAME = lname
 - 20 • CIF.EMAIL = email
 - CIFSERV.SRVCAT = service
 - CIFSERV.PASSWORD = service_password

The “single” handshake is used for services that all customers have access to, without login, enrollment, or registration requirements. An example of a “single” handshake site within the Internetbank is the public home page.

http(s)://<serviceURL>?<param1name>=<param1value>&...&<paramNname>=<paramNvalue>

http://home.Internetbank.com/Internet/users/users_home.htm

Example 4 - Return status of “Login” Handshake (second leg of the “tripe” handshake)

Once the remote services receive the login redirect, they reply with a redirect to the host server, indicating the status of the login request. The possible return values are:

- 5 OK - login successful
- FAILED - login did not match
- UNKNOWN - username not enrolled
- OTHER - service is having system problems

10 If the status is equal to FAILED, this indicates that the password data in the service provider’s database has been changed (for a variety of reasons). This event needs to be logged for security monitoring purposes. Then the USM will perform the registration process.

15 If the status is equal to UNKNOWN, this indicates the customer has never registered a userid/password for this service. Then the USM will also perform the registration process.

If the status is OTHER, then for some reason either the login was not processed properly by the remote system, or there were some remote system problem/errors. The customer will be directed to try again at a later time. This event will be logged for monitoring.

20 If the status is OK, then the User Session Manager needs to save the service’s local customer’s session ID. The USM handles the remote login process for the various services in a transparent manner to the customer. The USM keeps track of the various services the customers have entered during the session. It will store the remote local session IDS for each of the services a customer has successfully logged into. Thus, if

someone has successfully logged into a remote service during their customer session, the next time they select a link/tab to enter this service site, the USM knows they have been authenticated and will pass them directly to the “main” page of this site. This will limit the overhead of the “triple handshake” to once per customer session. If a remote service does not create session, then they can use whatever value they want to uniquely identify the customer. Preferably, the identifier value may not contain ampersands “&” and may not expose customer confidential data, such as social security number.

For example, the exception login may use the following format:

Hostname:xx, AppnName:xx, EventMsg:”EventClass:xxx, RemoteApp:xxx, UserID:xx, Source_ipaddr:xxx, SessionMgrID:xx, RemoteSessID:xx”, EventDescription:”error message”

For those services that do not include a registration process, examples of values that may be returned, from the login handshake, are “OK” or “OTHER”.

Example 5 - Second Leg of the “Triple” Handshake Specification

Services using the “triple handshake” may relay login status values back to the USM. For example, the first leg of the “triple handshake”, as described above may include a return URL parameter. Also, the remote services may append a session ID and a status to the end of this string and may have a complete signature for the second leg of the handshake.

For example, the resulting return redirect may look like:

https://www.Internetbank.com/listen?action=login&USMid=<USMsessionId>&service_name>&session=<local session id>&status<OK, FAILED, UNKNOWN or OTHER>

The return redirect may also look like:

<https://www.Internetbank.com/listen?action=login&Usmid=999999&service=BANKING&session=ababcdekduiekd&status=OK>

Example 6 - Customer navigation to Remote Service (final leg of the “triple” handshake)

After the return status has been evaluated and is successful, the remote session ID has been stored in the customers’ USM session, the customer may be redirected either to the registration process, a system problem message, or the production site. The customer navigation is preferably specified by the third leg of the “Triple” handshake.

After a successful remote login, the USM may redirect the customer to the service’s main page. The Internet bank system may have control of the outer frame and the top navigational bar. The various services’ pages may be hosted in the main bottom panel and may contain a left-hand navigation bar for local navigation. For example, a format for the redirect to the main page may be:

`https://www.<service_name>.com/<name of main page>?<param1name>=<param1value>&...&<paramName>=<paramNvalue>`

Also, the last leg of the “triple handshake” may be:

`https://banking.Internetbank.com/scripts/bankstart.exe?USMid=999999&session=ababcd
ekduiekd&service=BANKING`

In the case of a FAILED or UNKNOWN status, the USM may call the registration process to register (or re-register) the customer with the remote service. If the status is OTHER, then for some reason either the login was not processed properly by the remote system, or there were some remote system problem/errors. The customer may then be directed to try again at a later time. This event may be logged for monitoring.

Example 7 - Customer Service Registration

There are at least two kinds of data necessary for registering a customer with a remote service. The first is the unique userid and remote service password, the second is the data stored in the validation database necessary for registering a customer with a remote services databases.

The USM may use the CIF.ACN value as a unique userid. A remote password is generated using a series of algorithms specified by a data security server. Each remote service has a guarantee of not getting the same remote password as the other services for this customer because each service is specified a unique key that is used in the remote password generation process. These remote userids and passwords are unknown to the customers.

The exact data necessary to register a customer into the various services may vary depending upon the service. When a transparent service login fails with an UNKNOWN or FAILED status, then the registration process needs to contact the validation module Sanchez database to retrieve the information necessary for registration. This may be a two step process. For example, first the USM may contact the validation module with the CIF.ACN and the service name. The return values from this call are a list of column names of the data that has been flagged as necessary for registration. Then a second call may be made with the CIF.ACN value and the list of column names to retrieve the values necessary for registration.

A successful registration status may enable the User Session Manager to update the validation module with the remote password information. An unsuccessful registration status may cause the User Session Manager to give the customer a “try

again” message. If a remote service does not require registration they may never return the UNKNOWN or FAILED statuses to the login call, but only the “OK” or “OTHER” statuses.

Example 8 - Registration Handshake Specification

5 Registration redirects - If the login leg of the “triple handshake” returns a status value of FAILED or UNKNOWN, the USM may send a registration redirect to that service transparently. This registration call may preferably be called only once per the life of the customer as a member of the Internet Bank, not once per session. For example, the registration redirect may have the following format:

10 `https://<service_name's URL>/registration?customer_userid=<CIF.ACN>&service_password=<generatedremote_password>&●●●&<registration_nameN>=<nameN_value>&returnURL=www.Internetbank.com/listen?service=<service_name>&action=registration&USMsid=<User Session Manager session id>`

15 The generated remote password value may be generated dynamically for that customer and that service using a series of algorithms and unique seeds/key associated with each service. Therefore, all remote services may depend on receiving a different customer userid and service password combination for that customer than the other services.

20 Other parameter values may also be retrieved from the validation database and dynamically added to the URL. Typically, the USM may have no ability to control what parameter values are retrieved from the validation database. For example, the validation database may have a column that flags the values it stores as necessary for customer registration. These may be the values that are retrieved from the validation module. The remote service may also send an acknowledgment reply. As the example shows, the

reply may be the return URL parameter sent in the registration redirect with the addition of a local session ID and a status value.

www.Internetbank.com/listen?service=<service_name>&action=registration&USMsid=<User Session Manager session id>&status=<OK, FAILED, or OTHER>

- 5 If the reply contains the OK status value, then the remote password may be stored at the validation module and the USM may automatically start the “triple handshake” over again to transparently log the customer in. The event may be logged and the customer given a message indicating that there are problems accessing the remote site at this time. No data is updated the validation module.

10 **Example 9 - Logout Servlet**

- When a customer logouts or times out from the Internetbank host server, the USM may send a logout redirect to those remote services the customer has accessed during this session so that they may clean up their sessions. However, the remote service may choose to ignore this message. The USM may not receive a return from this redirect message. Thus this may be a message call without directing the customer’s browser to the remote services site. An exemplary format of the logout redirect may be:

https://www.<service_name>.com/logout?session=<remote_sid>

Example 10 - Dispatch Servlet

- For certain services, such as email, the various remote services may contact the USM directly (not via tab or link selection by the customer), so that the customer may be redirected to that service. An exemplary syntax for this servlet may be:

https://www.Internetbank.com/sessionManager/dispatch?service=<service_name>&<param1name>=<param1value>&...&<paramNname>=<paramNvalue>&fromService=<remote_service_name>

https://www.Interentbank.com/sessionManager/dispatch?service=email&acctNum=<customer's acctnumber>&fromService=<remote_service_name>

The dispatch servlet may follow the following business logic to determine customer navigation:

- 5 a) Check to ensure the user has authenticated with Internetbank host server. If not, the USM may direct the user to a marketing/demo site for this service;
- b) If the customer has been validated, and the customers session table shows they have already been successfully logged into this remote service during the current session, the USM may direct them to the remote site's "main" page;
- 10 c) If the customer has been validated and has not been logged into this remote service yet, and the CIFSERV.STATUS value for this service is 0 or if the customer is not enrolled in this service, the USM may direct the user to the marketing/demo site;
- 15 d) If the customer has been validated and has not been logged into this remote service yet, and is enrolled with a CIFSERV.STATUS value of 1 for this service, the USM may do the login redirect; and
- 20 e) If the customer has been validated and has not been logged into this remote service yet, and has a CIFSERV.STATUS value of 2, the USM may send them to a Generic Message site with a message, such as "Your application is being processed. You will be notified when your account is activated."

CheckLogin servlet - If a remote service detects that a user entered their site directly, or if their own remote session timed out while the customer was active elsewhere on the Internet bank host server, they may want the transparent login to take place again to initiate a new local session. In this case, they can call a checkLogin
25 servlet. The checkLogin servlet may:

- f) Check to ensure the user has authenticated with the host server. If not, the USM may direct the user to the marketing/demo site for this service;
- 30 g) If the customer has been validated, and the CIFSERV.STATUS value for this service is 0 or if the customer is not enrolled in this service, the USM may direct the user to the marketing/demo site;

- h) If the customer has been validated and is enrolled with a CIFSERV.STATUS value of 1 for this service, the USM may do the login redirect, even if they have already entered this site during their current session;
- 5 i) If the customer has been validated and has an CIFSERV.STATUS value of 2, the USM will send them to the Generic Message site with the message, "Your application is being processed. You will be notified when your account is activated."

Example 11 - Change Password Servlet

The USM may include password functionality. On a change password screen, a
10 customer may be allowed to select a new password (not a new username). Typically, they may provide a username, an old password, and a new password. The username and old password may be verified at a validation module to be correct. If this verification succeeds, the USM may check that the new password passes a set of rules to ensure the password is strong enough. If this succeeds, then the USM will update the primary
15 password at validation module for this customer and return a successful changed password message. In case of any failures, the customers are notified the password was not successfully changed.

Customers with disabled accounts from for example 3 or more
username/passwords failures, may not change their password until a predetermined time
20 such as a 24 hour period has elapsed and their account is enabled.

Example 12 - Vanity Servlet

The vanity servlet is a class used to execute vanity URLs. For instance, in the URL "www.Internetbank.com/login", "www.Internetbank."com" is the base URL and "login" is the vanity URL. The vanity URL can be created by using classes as explained
25 below.

A “VanityReload” class is a startup class that can be initialized every time weblogic is started. TheVanityReload class is responsible for reloading a vanity.properties file. The vanity.properties file is the file that is initially loaded during initial USM server startup. The vanity.properties file may be modified by adding and deleting URLs. It is stored in the server’s memory and used by the vanity servlet for any vanity request. In order to add a new URL to the vanity.properties file, the procedure may be performed as explained below.

To add a new vanity URL “abc”, i.e http://www.Internetbank.com/abc, an abc.uri property is required. For example, abc.uri=/sessionManager/dispatch?service=apply sends http://www.Internetbank.com/sessionManager/dispatch?service=apply to the vanity URL. Some of the optional properties that can be set using abc.urlBase can include overriding the default urlbase e.g. abc.urlBase=http://promo.Internetbank.com/ abc.uri=abc.htmlwill send to http://promo.Internetbank.com/abc.html instead of http://www.Internetbank.com/abc.html.

The ‘abc’.parameters can specify what parameters should be appended to abc.uri. If this (abc.params) property is set, corresponding individual parameter’s properties should be set. For example, the following properties:

abc.uri=abc.html

abc.params=cell,promo,click_id,brand

abc.cell=6WGD, abc.promo=VWG9DWG51,

abc.click_id=%j

abc.brand=WING

would create and redirect to

http://www.Internetbank.com/abc.html?cell=6WGD&promo=VWG9DWG51&click_id=

%j&brand=WING

An abc.expirydate property can be used to tell when the vanity URL expires.

Format YYYYMMDD, for example, abc.expirydate=20000416. An abc.offerExpired.url is set to the URL where it is redirected to when vanity URL expires e.g

5 abc.offerExpired.url=http://www.wingspanbank.com/sorry.html

The default urlBase is which ever region the server is running under.

If the server is running in QA port 80 the default urlBase will be

http://wwwqa.Internetbank.com/.

10 **Example 13 - Customer Messaging**

The USM may also provide a generic message screen where informative messages will be displayed for the customers depending on some error condition occurring. For example, messaging conditions may include:

- Invalid Login attempt (*)
- 15 • Disabled account (*) - exceeded 3 maximum failed login attempts
- Remote Service failure (*) - if login or registration fails due to "OTHER" reasoning (system, network, or dB failure)
- Remote Service unknown (*) - if service name is not known to the USM and there is no valid redirects available
- 20 • System failure (*) - if there are some system problems that arise.
- Successful Change Password
- Invalid Change Password attempt (*) - if the username and old password do not match what is in Sanchez
- 25 • Disabled Change Password attempt (*) - if the username and old password had or becomes disabled during Change Password process
- Unsuccessful Change Password attempt (*) - if there were some system problems, SQL update problems during the Change Password process
- Pending Account Status - if the customer's CIFSERV.STATUS value is equal to 2.

In the (*) conditions above, the events are logged in the format requested by the
30 Data Security server. These logged events may be written to logs on an hourly or other

basis and there are processes searching these logs to generate reports. This file needs to be augmented to trigger alerts automatically.

Example 14 - Customer Branding/Top Navigation Bar

The User Session Manager may also have the capability to provide customized
5 top navigation bars depending on how a customer enters the Internet banking service, whether they go directly to host server or whether they link to the Internet banking service from a partnered site, such as an Internet search engine.

Since the USM repaints the top navigation bar frequently during a customers' session, a mechanism is included to capture the brand, when a customer comes in front a
10 partnered site, and retain it for the life of the customers host server session. For example, the USM may own the global outer frame, and all navigation may be directed through the USM.

Thus, when a customer navigates to the host server, the USM may check to see if there exists a valid customer session. If not, the USM may create a sessions, store the
15 branding ID in the session and pass the rest of the query string parameters along to the designated service. All services may need to be notified that more data may be passed to them in the redirects and they may need to parse the data, or at least the branding ID along to all page redirects, within their systems as well as within the Internet bank system.

20 The USM may take some of its internal functions and make them into services, such as login. For example, the ad URL may be specified by a partner, when the

customized top navigation bar is displayed. In one embodiment, customers of a search engine server can access the Internet Banking host server at least at three places.

An ad generator module may be employed to prevent display of competing ads in the top navigation bar to the partnered site or brand.

5 **Example 15 - USM OFX Interface**

Preferably, an Internet banking customer, such as with an access account such as a Quicken account, or with the vanity servlet, or other mechanism may be able to download all of their account data from a single button click. One way to accomplish this may include configuring the access account or vanity.properties file to access the Internet banking OFX server with an Internet banking username and password. The Internet banking OFX server would then need to contact the USM to:

1. Perform the customer login to Internet bank service transparently;
2. The list of accounts retrieved from the validation module would have to have an indicator that flags it as one of the customer's accounts they want data automatically download;
3. The USM would then need to transparently log into the services that maintain the data for these accounts and retrieve the data (this could be by contacting an OFX server for each remote service);
4. The USM would then return this data to the Internet bank OFX server
5. The Internet bank OFX server may return the data to the OFX server and the data downloaded to the customer.

Example 16 - Email

A separate server may be hosting the email services for the Internet banking system. For example, there may be links to email at various locations throughout the system so customers can email their questions or concerns. The required pieces of data for email are first name, last name, email address and optionally account number. If it is

the Internet banking host server contacting the email service, the account number will be their Internet bank account number. For the remote services, such as brokerage, they may need to contact the USM so the customer can get redirected to the email service.

The USM may also retrieve additional data values from a response to the validation customerLogin query. If the customer has not logged in, there will be no values for first name, last name, or email. At this point, the bottom frame may be replaced with the email service. When the customer is done their email clicks submit, the email service may redirect them to the dispatch servlet to direct the customer back to the remote services' main page. Notice that the service name variable for the service=broker below may be the from Service value in the last part of the email redirects. The email service redirect may be: www.Internetbank.com/sessionManager/dispatch?service-broken.

Additional advantages features and modifications will readily occur to those skilled in the art. Therefore, the invention is not limited to the specific details in the representative embodiments shown and described above. Accordingly, various modifications may be made without departing from the spirit and scope of the general inventive concept as defined by the appended claims.